UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,420	01/05/2004	Gregory Gordon Rose	030010	3858

23696 7590 04/01/2009

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
KANE, CORDELIA P	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
04/01/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	10/752,420	ROSE ET AL.	
	Examiner	Art Unit	
	CORDELIA KANE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28,50 and 51* is/are pending in the application.

4a) Of the above claim(s) *29-49* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28,50 and 51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election without traverse of claims 1 – 28, 50 and 51 in the reply filed on January 19, 2009 is acknowledged.

Response to Arguments

2. Applicant's arguments with regards to 35 USC 101 have been fully considered but they are not persuasive. Applicant argues that the specification defines the embodiments to include hardware. However, the specification also defines that the embodiments may be implemented in software ([0064]). Software does not fall into one of the statutory categories.

3. Applicant's arguments with respect to claims 1 – 28, 50 and 51 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 4, 22 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear if the first private key is disabled when the second private key is re-created or if when the second private key is used for authentication. It appears that the independent and dependent claims are contradictory.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> a. Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 14 - 21,and 40 - 42 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In the specification applicant defines the means to include software only [0064].

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 1 – 9, 11 – 14, 16 – 28, 50 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis's US Patent 5,761,306, and further in view of Boneh et al's US Publication 2003/0081785 A1. Referring to claims 1, 14 and 22, Lewis teaches:

b. Creating a first private key and corresponding public key (column 6, lines 14-16).

c. Creating a second private key associated with the first private key and creating a second public key corresponding to the second private key (column 6, lines 14-17).

d. Disabling the first private key when the second private key is used (column 3, lines 25-26).

e. Transmitting the second public key concurrent with the first public key (column 3, lines 23-25, column 4, lines 12-14).

f. Using the first private key for authentication (column 8, lines 40-49).

10. Lewis fails to teach a wireless network, or distributing a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Boneh teaches that it is desirable to protect the private key and to protect the key by distributing it among a plurality of different entities, and then constructing the key by requesting the shares from the entities (page 14, paragraph 253). Boneh also discloses that communications include medium such as radio broadcasting, and wireless communications (page 5, paragraph 57). Lewis and Boneh are analogous art because they are from the same field of endeavor, encryption. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Boneh before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Boneh. The suggestion/motivation for doing so would have been to protect the private key (page 14, paragraph 253).

11. Referring to claims 2 and 23, Boneh teaches:

g. Creating at least two shares of the second private key at the device (page 14, paragraph 253).

h. Outputting each share to a different entity (page 14, paragraph 253) wirelessly (page 5, paragraph 57).

12. Referring to claims 3, 16, and 24, Lewis teaches using the second private key for authentication (column 7, lines 31-37, column 8, lines 40-49). Boneh teaches re-creating the private key at the device using the plurality of shares (page 14, paragraph 253). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Boneh before him or her, to modify the system of Lewis to include the private key distribution of Boneh. The suggestion/motivation for doing so would have been to protect the private key (page 14, paragraph 253).

13. Referring to claims 4 and 25, Lewis teaches disabling the first private key when the second private key is used for authentication of the device (column 3, lines 25-26).

14. Referring to claims 5 and 17, Lewis teaches:

i. Creating a third private key associated with the second private key, and creating a third public key corresponding to the third private key (column 7, lines 31-37).

j. Outputting the third public key (column 7, lines 59-65).

15. Referring to claim 6, Lewis teaches using the third private key for authentication (column 7, lines 31-37, column 8, lines 40-49). Boneh teaches outputting the private key once such that it can be recreated (page 14, paragraph 253). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Boneh before him or her, to modify the system of Lewis to include the private key distribution of Boneh. The suggestion/motivation for doing so would have been to protect the private key (page 14, paragraph 253).

16. Referring to claim 7, Lewis teaches that the second private and public keys are created independently from the first private and public keys (column 7, lines 59-60).

17. Referring to claims 8 and 18, Lewis teaches:

k. Creating a third private key associated with the second key and creating a third public key corresponding to the third private key (column 7, lines 31-37).

l. Creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key (column 7, lines 31-37).

m. Outputting the third and fourth public keys (column 7, lines 59-65).

18. Lewis fails to teach outputting the fourth private key once such that it can be recreated. However, Boneh teaches outputting the private key once such that it can be recreated (page 14, paragraph 253). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Boneh before him or her, to modify the system of Lewis to include the private key distribution of Boneh. The suggestion/motivation for doing so would have been to protect the private key (page 14, paragraph 253).

19. Referring to claim 9, Lewis teaches:

n. Disabling use of the second private key for authentication (column 3, lines 25-26).

o. Using the third private key for authentication (column 8, lines 40-49).

p. Using the fourth private key for authentication (column 8, lines 40-49).

20. Lewis fails to teach recreating the fourth private key. However, Boneh teaches recreating the private key (page 14, paragraph 253). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Boneh before him or her, to modify the system of Lewis to include the private key distribution of Boneh. The suggestion/motivation for doing so would have been to protect the private key (page 14, paragraph 253).

21. Referring to claims 11, 19, and 26, Lewis discloses:

q. Receiving a first public key (column 10, lines 1-4).

r. Receiving a second public key concurrent with receipt of the first public key, the second public key associated with the first public key (column 10, lines 1-4), wherein the second public key has a corresponding second private key (column 6, lines 14-17), and the first private key is disabled when the second private key is recreated (column 3, lines 25-26).

s. Using the first public key for authentication (column 8, lines 40-49).

t. Using the second public key for authentication if the first public key fails (column 8, lines 58-64).

22. Lewis fails to teach a wireless network, or distributing a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Boneh teaches that it is desirable to protect the private key and to protect the key by distributing it among a plurality of different entities, and then constructing the key by requesting the shares from the entities (page 14, paragraph 253). Boneh also discloses that communications include medium such as radio broadcasting, and wireless

communications (page 5, paragraph 57). Lewis and Boneh are analogous art because they are from the same field of endeavor, encryption. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Boneh before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Boneh. The suggestion/motivation for doing so would have been to protect the private key (page 14, paragraph 253).

23. Referring to claims 12, 20 and 27, Lewis teaches receiving a third public key from the device, the third public key associated with the second public key (column 7, lines 31-37), if the first public key fails and the second key results in successful authentication (column 8, lines 58-64).

24. Referring to claims 13, 21, and 28, Lewis teaches a third public key and a fourth public key from the device (column 7, lines 31-37), if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second key (column 8, lines 58-64).

25. Referring to claim 50, Lewis teaches:

u. A processor configured to generate a first private key and corresponding first public key, the processor configured to generate a second private key associated with the first private key and to create a second public key corresponding to the second private key (column 6, lines 14-17).

v. A storage medium coupled to the processor to store the first private key (column 6, lines 14-17).

w. A transmitter to output the second public key to the device concurrent with outputting the first public key (column 10, lines 1-4) and disable the first private key when the second private key is created (column 3, lines 25-26).

x. Wherein the processor uses the first private key for authentication of the device (column 8, lines 40-49).

26. Lewis fails to teach a wirelessly outputting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Boneh teaches that it is desirable to protect the private key and to protect the key by distributing it among a plurality of different entities, and then constructing the key by requesting the shares from the entities (page 14, paragraph 253). Boneh also discloses that communications include medium such as radio broadcasting, and wireless communications (page 5, paragraph 57). Lewis and Boneh are analogous art because they are from the same field of endeavor, encryption. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Boneh before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Boneh. The suggestion/motivation for doing so would have been to protect the private key (page 14, paragraph 253).

27. Referring to claim 51, Hollis teaches:

y. A receiver configured to receive a first public key from a device and receiving a second public key from the device concurrent with receipt of the first public key, the second public key associated with the first public key (column 10,

lines 1-4), wherein the second public key has a corresponding second private key (column 6, lines 14-17), and the first private key is disabled when the second private key is recreated (column 3, lines 25-26).

z. A storage medium coupled to the receiver configured to store the first and second public keys (column 10, lines 1-4).

aa. A processor coupled to the receiver, the processor configured to use the first public key for authentication (column 8, lines 40-49), the processor configured to use the second public key for authentication if the first public key fails (column 8, lines 58-64).

28. Lewis fails to teach a wirelessly outputting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Boneh teaches that it is desirable to protect the private key and to protect the key by distributing it among a plurality of different entities, and then constructing the key by requesting the shares from the entities (page 14, paragraph 253). Boneh also discloses that communications include medium such as radio broadcasting, and wireless communications (page 5, paragraph 57). Lewis and Boneh are analogous art because they are from the same field of endeavor, encryption. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis and Boneh before him or her, to modify the system of Lewis to include the wireless communication and private key distribution of Boneh. The suggestion/motivation for doing so would have been to protect the private key (page 14, paragraph 253).

29. Claims 10, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Boneh, as applied above, and further in view of Brennan et al's US Patent 5,675,649.

30. Referring to claim 10, Lewis in view of Boneh teaches all the limitations of the parent claim. Lewis in view of Boneh fails to teach preventing retransmission of the second private key. However, Brennan teaches that after the key shares are distributed that secure computer system is shut down such that the key information cannot be reconstructed at the secure computer system (column 2, lines 16-31). Lewis and Boneh and Brennan are analogous art because they are from the same field of endeavor, encryption. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis in view of Boneh before him or her, to modify the system of Lewis in view of Boneh to include destroying the key of Brennan. The suggestion/motivation for doing so would have been to prevent the computer from reconstructing the key (column 2, lines 28-31).

31. Referring to claim 15, Lewis in view of Boneh teaches all the limitations of the parent claim, in addition to creating at least two shares of the second private key at the device and outputting each share to a different entity (Boneh, page 14, paragraph 253) wirelessly (Boneh, page 5, paragraph 57). Lewis in view of Boneh fails to that subsequent outputting of the second private key is prevented. However, Brennan teaches that after the key shares are distributed that secure computer system is shut down such that the key information cannot be reconstructed at the secure computer

system (column 2, lines 16-31). Lewis and Boneh and Brennan are analogous art because they are from the same field of endeavor, encryption. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Lewis in view of Boneh before him or her, to modify the system of Lewis in view of Boneh to include destroying the key of Brennan. The suggestion/motivation for doing so would have been to prevent the computer from reconstructing the key (column 2, lines 28-31).

Conclusion

32. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA KANE whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. K./
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432